CLAIMS

1. A data processing method performed by a means to be authenticated for holding first authentication use data generated by encryption using key data and an authenticating means for holding the key data, comprising:

a first step by which the means to be authenticated provides key designation data designating the key data to the authenticating means;

a second step by which the authenticating means performs encryption using the key data designated by the key designation data received at the first step to generate second authentication use data;

a third step by which the means to be authenticated uses the first authentication use data for authentication and uses the second authentication use data for authentication; and

a fourth step by which the authenticating means executes processing related to the key data when the authentication at the third step decides that the first authentication use data and the second authentication use data are the same.

2. A data processing system comprising:

a means to be authenticated for holding first authentication use data generated by encryption using key

data and

an authenticating means for holding the key data, wherein

the means to be authenticated provides key designation data designating the key data to the authenticating means,

the authenticating means performs encryption using the key data designated by the key designation data received from the means to be authenticated to generate second authentication use data,

the means to be authenticated uses the first authentication use data for authentication and the authenticating means uses the second authentication use data for authentication, and

the authenticating means executes the processing related to the key data when the authentication decides that the first authentication use data and the second authentication use data are the same.

3. A data processing method where an authenticating means holding predetermined key data performs authentication together with a means to be authenticated holding first authentication use data generated by encryption using the key data, comprising:

a first step of receiving key designation data for designating the key data from the means to be

authenticated;

a second step of using the key data designated by the key designation data received at the first step for encryption to generate second authentication use data;

a third step of using the second authentication use data generated at the second step for authentication with the means to be authenticated using the first authentication use data for authentication; and

a fourth step of executing processing related to the key data when the authentication at the third step decides that the first authentication use data and the second authentication use data are the same.

4. A data processing method as set forth in claim 3, further comprising, in the fourth step, executing the functions of the authenticating means authorized to the means to be authenticated related to the key data or accessing the data held by the authenticating means.

5. A data processing method as set forth in claim 3, further comprising, when the authentication use data is generated by using a plurality of different key data, in the fourth step, executing a plurality of processings related to the plurality of key data.

6. A data processing method as set forth in

claim 5, further comprising, in the fourth step, executing a plurality of processings including the functions of the authenticating means and access to the data held by the authenticating means relating to the plurality of key data.

7. A data processing method as set forth in claim 3, further comprising, in the fourth step, accessing the plurality of data modules related to single key data when the authenticating means holds a plurality of data modules as data.

8. A data processing method as set forth in claim 3, further comprising, in the first step, receiving the key designation data read by a device of the means to be authenticated from an integrated circuit holding the first authentication use data and the key designation data.

9. A data processing method as set forth in claim 3, wherein the first authentication use data is data generated by encrypting predetermined data by using the key data.

10. A data processing method as set forth in claim 9, wherein the first authentication use data is data generated by encrypting data obtained by encrypting the predetermined data by using the key data by further using tamper-proofing key data managed by the management

side.

11. A data processing system for authentication with a means to be authenticated holding first authentication use data generated by encryption using predetermined key data and holding the key data, comprising:

an inputting means for inputting key designation data for designating the key data from the means to be authenticated;

an authenticating means for using the key data designated by the key designation data received by the inputting means for encryption to generate second authentication use data and using the second authentication use data for authentication with the means to be authenticated using the first authentication use data for authentication; and

a controlling means for executing processing related to the key data when the authentication by the authenticating means decides that the first authentication use data and the second authentication use data are the same.

12. A program to be executed by a data processing system for authentication with a means to be authenticated holding first authentication use data generated by encryption using predetermined key data and

holding the predetermined key data, comprising:

a first routine of receiving key designation data for designating the key data from the means to be authenticated;

a second routine of encryption using the key data designated by the key designation data received by the first routine to generate second authentication use data;

a third routine of using the second authentication use data generated by the second routine for authentication with the means to be authenticated using the first authentication use data for authentication; and

a fourth routine of executing processing related to the key data when the authentication in the third routine decides that the first authentication use data and the second authentication use data are the same.

13. A data processing method performed by a means to be authenticated when an authenticating means holding key data uses key data designated from the means to be authenticated holding the first authentication use data for encryption to generate second authentication use data, uses the second authentication use data for authentication with the means to be authenticated, and performs processing related to the key data conditional

on the authentication confirming that the first authentication use data and the second authentication use data are the same, comprising:

a first step of providing key designation data for designating the key data used when generating first authentication use data based on the predetermined generation method to the authenticating means;

a second step of using the first authentication use data for authentication with the authenticating means; and

a third step of making the authenticating means perform processing related to the key data based on the results of the authentication at the second step.

14. A data processing method as set forth in claim 13, wherein the means to be authenticated reads and holds the first authentication use data and the key designation data from a predetermined integrated circuit.

15. A data processing method as set forth in claim 13, further comprising, in the third step, making the authenticating means execute the functions of the authenticating means authorized to the means to be authenticated related to the key data or accessing the data held by the authenticating means.

16. A data processing method as set forth in claim 13, further comprising, when defining a group

comprising a plurality of authenticating means,

in the first step, collectively providing the key designation data to the group and,

in the third step, collectively making the group perform the processings related to the key data.

17. A data processing method as set forth in claim 13, further comprising a fourth step of providing a screen displaying an image corresponding to the authenticating means for performing the processing by using a plurality of different patterns in accordance with the operation state of the authenticating means.

18. A data processing method as set forth in claim 17, further comprising, in the fourth step, providing a screen displaying an image corresponding to the authenticating means by a pattern enabling identification of whether or not the authenticating means already confirmed the legitimacy of the means to be authenticated by the authentication in the second step.

19. A data processing system forming a means to be authenticated when an authenticating means holding key data uses key data designated from the means to be authenticated holding the first authentication use data for encryption to generate second authentication use data, uses the second authentication use data for authentication with the means to be authenticated, and

performs processing related to the key data conditional on the authentication confirming that the first authentication use data and the second authentication use data are the same, comprising:

a first means for providing key designation data for designating the key data used when generating first authentication use data based on the predetermined generation method to the authenticating means;

a second means for using the first authentication use data for authentication with the authenticating means; and

a third means for making the authenticating means perform processing related to the key data based on the results of the authentication of the second means.

20. A program to be executed by a data processing system forming a means to be authenticated when an authenticating means holding key data uses key data designated from the means to be authenticated holding the first authentication use data for encryption to generate second authentication use data, uses the second authentication use data for authentication with the means to be authenticated, and performs processing related to the key data conditional on the authentication confirming that the first authentication use data and the second authentication use data are the same, comprising:

a first routine of providing key designation data for designating the key data used when generating first authentication use data based on the predetermined generation method to the authenticating means;

a second routine of using the first authentication use data for authentication with the authenticating means; and

a third routine of making the authenticating means perform processing related to the key data based on the results of the authentication of the second means.